**3GPP TSG-SA3 Meeting SA3#112 *S3-234355***

**Goteborg, Sweden, 14 - 18 Aug 2023**

|  |
| --- |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1786** | **rev** | **-** | **Current version:** | **18.2.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  |  Security aspects of enablers for Network Automation for 5G |
|  |  |
| ***Source to WG:*** | China mobile, Nokia, Nokia Shanghai Bell, Ericsson, China Telecommunications, Intel, Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eNA\_Ph3\_SEC |  | ***Date:*** | 2023-04-10 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | To capture the Security aspects of enablers for Network Automation for 5G - phase 3 |
|  |  |
| ***Summary of change:*** | How the work on the eNA phase 3 security study can be included in TS 33.501. |
|  |  |
| ***Consequences if not approved:*** | Enhanced support of eNA will not have necessary security aspects specified. |
|  |  |
| ***Clauses affected:*** | Annex X |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** | S3-232189, S3-233266, S3-234282 |

\*\*\* BEGIN CHANGES \*\*\*

Annex X (normative):
Security aspects of enablers for Network Automation (eNA) for the 5G system (5GS)

# X.x Protection of data and analytics exchange in roaming case

## X.x.1 General

The protection of data and analytics exchange in roaming case including authorization and anonymization of data/analytics:

- Authorization at data and analytics level is enforced by the roaming entry NWDAF producer. The parameters used by NWDAF service consumer to request/subscribe to the services provided by NWDAF producer are defined in TS 23.288 [105], clause 6.1.5. Accordingly, the operator authorization policies can be configured locally in the NWDAF producer. Also, when the NWDAF in one PLMN requests an access token from the NRF in the peer PLMN, the access token request and the access token claims may contain the Analytics ID.

- The roaming entry NWDAF producer is responsible to control the amount of exposed data/analytics and to abstract or hide internal network aspects in the exposed data/analytics. The corresponding mechanisms used to restrict the data/analytics and/or anonymization are subject to the implementation.

## X.x.2 Procedure for protection of analytics exchange in roaming case

### X.x.2.1 Policies configured locally in Roaming entry NWDAF producer



Figure X.x.2.1-1: Protection of analytics exchange when policies configured locally in Roaming entry NWDAF

Pre-requisites:

- Roaming entry NWDAF producer, i.e. NWDAFp shall be pre-configured with a list of allowed analytics per PLMN.

- If token-based authorization is used, NWDAFc shall have acquired an access token from the PLMN2 to consume the services exposed in Nwdaf\_RoamingAnalytics\_Subscribe/Request APIs.

Step 1: NWDAFc sends Nnwdaf\_RoamingAnalytics\_Subscribe/Request message to NWDAFp to request analytics.

Step 2: The roaming entry NWDAFp shall verify the service request, including verifying token and the visited PLMN ID and determine whether the requested analytics are allowed to be exposed to NWDAFc in PLMN1 by pre-configured policies.

Step 3: The roaming entry NWDAFp shall apply the security policies per consumer (PLMN) to the requested analytics and decide on their anonymization, restriction or desensitization based on operator’s policy.

NOTE: The anonymization, restriction or desensitization mechanisms of analytics are left for implementation.

Step 4: NWDAFp returns the requested and processed analytics to NWDAFc.

### X.x.2.2 Policies configured as extended claims in access token



Figure X.x.2.2-1: Protection of analytics exchange when policies configured as extended claims in access token

Pre-requisite:

- The producer NRF has the NF profile of the NF Service Producer including the list of allowed Analytics ID(s) per PLMN. According to TS 29.510 [68] clause 5.2.1, the NF profile can be configured in the NRF by other means such as O&M.

Step 1: NWDAFc sends an access token request to the consumer NRF as specified in clause 13.4.1. The access token request may contain the Analytics ID.

Step 2: vNRF forward the token request message to hNRF as specified in clause 13.4.1.

Step 3: The home network hNRF shall verify the token get request as specified 13.4.1, then determine whether the requested analytics implied by the Analytics ID(s) can be obtained by the visited PLMN according to the allowed analytics ID(s) of the visited PLMN.

Step 4: If the verification success, hNRF issue the token as specified in clause 13.4.1.The allowed Analytics ID(s) of the visited PLMN may be included in the token.

Step 5: The vNRF forward the Token\_Get Response to NWDAFc as specified in clause 13.4.1.

Step 6: If the requested analytics is within the claim of token, the NWDAFc sends Nnwdaf\_RoamingAnalytics\_Subscribe/Request with the issued token to NWDAFp,

Step 7: The roaming entry NWDAFp verifies the service request, including verifying token as specified in clause 13.4.1, and whether the requested analytics are consistent with the Analytics ID(s) in the token.

Step 8: The roaming entry NWDAFp shall apply the security policies per consumer (PLMN) to the requested analytics and decide on their anonymization, restriction or desensitization based on operator’s policy.

NOTE: The anonymization, restriction or desensitization mechanisms of data / analytics are left for implementation.

Step 9: Roaming entry NWDAFp returns the requested and processed analytics to NWDAFc.

# X.y Authorization of selection of participant NWDAF instances in the Federated Learning group

The authorization for selecting participant NWDAF instances in the Federated Learning (FL) group uses token-based authorization as specified in clause 13.4.1, with the following additions.

Figure X.9-1 depicts the authorization mechanism for NWDAF containing MTLF acting as FL Server to initiate the Federated Learning process on the NWDAF containing MTLF(s) acting as FL Client(s). The authorization is based upon the FL capability type (FL server or FL client) provided by the NWDAF containing MTLF acting as FL server during registration, and the Analytics ID and Interoperability Indicator per Analytics ID provided by the NWDAF containing MTLF acting as FL client during registration.

Editor’s note: The use of Service area and Availability time requirement for authorization is FFS.



Figure X.y-1: FL Authorization for selecting participant NWDAF instances

Step 1a. The NWDAF containing MTLF acting as FL client registers to the NRF with its FL related information, including supported FL capability (FL client), Analytics ID(s) and Interoperability Indicator per Analytics ID as described in clause 5.2 of TS 23.288.

Step 1b. The NWDAF containing MTLF acting as FL server registers to the NRF with its FL capability (FL Server).

Step 2. The NWDAF containing MTLF acting as FL server (NF Service Consumer) sends a discovery request to NRF and receives the available NWDAFs containing MTLF acting as FL client(s) (NF Service Producer) as a response, as specified in clause 6.2C.2.1 of TS 23.288 [105].

Step 3. The NWDAF containing MTLF acting as FL server (NF Service Consumer) sends an access token request to the NRF as specified in clause 13.4.1. The access token request may contain the Analytics ID for the requested Federated Learning process.

Step 4. The NRF authorizes the NWDAF containing MTLF acting as FL server (NF Consumer) based upon the information received in Step 1b, and after verifying that the Server NWDAF’s Vendor ID is included in the Interoperability Indicator for the requested Analytics ID provided in Step 1a. If the authorization succeeds, NRF generates the access token(s) as specified in clause 13.4.1. The access token claims may include the Analytics ID for the request Federated Learning process.

NOTE: Fine-grained authorization can be done locally at the NWDAFs containing MTLF acting as FL client(s) (NF Service Producer).

Step 5a, 5b. The NRF sends the access token to the NWDAF containing MTLF acting as FL Server, or rejects the request in case of failed authorization, as described in clause 13.4.1.

Step 6. The NWDAF containing MTLF acting as FL server sends the service request to the NWDAF(s) containing MTLF acting as FL client with the access token received in Step 5a. along with the Analytics ID information for which the FL process is to be performed, as described in TS 23.288 [105].

Step 7, 8. The NWDAF containing MTLF acting as FL client (NF Service Producer) verifies the received access token as specified in clause 13.4.1. In case of successful access token verification, the NWDAF containing MTLF acting as FL client sends a success response to the NWDAF containing MTLF acting as FL server, as described in TS 23.288 [105].

Step 9. After a successful response from the NWDAF(s) containing MTLF acting as FL client, the NWDAF containing MTLF acting as FL server initiates the Federated Learning process as described in TS 23.288 [105].

Authorization of the NWDAF containing MTLF acting as FL client is implicit, since it can join a Federated Learning group only when selected by the NWDAF containing MTLF acting as FL server.

# X.z Security for AI/ML model storage and sharing

The detailed procedure for secured and authorized AI/ML model sharing between different vendors is depicted in Figure X.10-1:

****

 Figure X.z-1: Secured and authorized AI/ML model sharing between different vendors

0a. NF Service producer i.e. NWDAF containing MTLF registers its NF profile in the NRF with ML Model Interoperability indicator per Analytics ID as described in clause 5.2 of TS 23.288 [105]. The ML Model Interoperability indicator is a list of NWDAF providers (vendors) that are allowed to retrieve ML models from this NWDAF containing MTLF.

0b. NF Service consumer e.g., NWDAF containing AnLF registers at the NRF including its Vendor ID,

Editor's Note: The inclusion of Interoperability indicator of NFc and Vendor ID of NFc are needed for authorization is ffs.

0c. The model is stored in encrypted format unless both the AI/ML model producer (NWDAF MTLF) and storage platform (ADRF) are part of the same system and belong to the same vendor and operator security domain.

 Storage of the model in encrypted format can be required by the trust model established to store and share AI/ML models. The trust model between AI/ML NF producer (NWDAF MtLF), storage platform (ADRF) and NF consumer (e.g., AnLF) is to be determined during the implementation phase among operator and the providers of the different platforms (MTLF, AnLF, ADRF). How the model is encrypted is vendor specific. Key distribution is not specified in this document.

1. NWDAF containing MTLF triggers the Nadrf\_MLModelManagement\_StorageRequest as described in TS 23.288 [105], optionally including an allowed NFc list. The absence of allowed NFc list indicates that only the MTLF which stored the model is allowed to retrieve the model.

2. ADRF sends the response to NWDAF containing MTLF as described in TS 23.288 [105].

3. NF Service consumer e.g., NWDAF containing AnLF performs Nnrf\_NFDiscovery\_Request operation with the requested Analytics ID to select a suitable NF Service Producer e.g., NWDAF containing MTLF.

4a. NF Service consumer e.g., NWDAF containing AnLF requests an access token from the NRF using the Nnrf\_AccessToken\_Get request operation. The token request message contains, besides the parameters described in clause 13.4.1.1.2, the Vendor ID of NWDAF containing AnLF and the Analytics ID.

4b. NRF checks whether the NWDAF containing AnLF is authorized to access the requested service in NWDAF containing MTLF and verifies that the NF Consumer's Vendor ID is included in the NWADF containing MTLF 's interoperability indicator for the Analytics ID and grants the token (token1), based on the vendor ID provided by the NF consumer during registration.

 5. NF Service Consumer performs Nnwdaf\_MLModelProvision (Analytics ID, Vendor ID and token1) service operation at the NWDAF containing MTLF to retrieve ML models for the Analytics ID.

 6a. The NWDAF containing MTLF authenticates the NF Service Consumer and verifies the access token as specified in the clause 13.4.1.1.2 and ensures that the Analytics ID is included in the access token. If verification is successful, NWDAF containing MTLF determines the ML model to be shared for the requested Analytics ID and stored the NF instance ID of NWDAF containing AnLF as part of allowed NF instance list for the ML model.

 6b. If the determined ML model is stored in ADRF, and if the NF Service Consumer is not yet in the allowed NFc list stored at the ADRF, the NWDAF containing MTLF triggers the update of Nadrf\_MLModelManagement\_StorageRequest at the ADRF, with NF ID of NWDAF containing MTLF and Model ID, adding the NF Service Consumer to the allowed NFc list. The ADRF verifies that the requesting NWDAF containing MTLF is same as the one that stored the model. Then, ADRF stores the allowed NF instance list for the ML model referenced by the Model ID.

Editor's Note: New service operation Nadrf\_MLModelManagement\_StorageRequest Update needs to be defined by SA2.

Editor's Note: How the MTLF and ADRF can identify which list of allowed NF consumers belongs to which model stored in the ADRF (e.g. by Storage Transaction ID) is ffs.

 6c. ADRF sends the response to NWDAF containing MTLF which contains Model ID.

Editor's Note: How the AnLF retrieve the model via MTLF should be align with SA2 and the diagram should be update accordingly.

 7. NWDAF containing MTLF sends Nnwdaf\_MLModelProvision Notify to the NF Service Consumer with Model ID, the address of the determined ML model, which can be either the one stored in NWDAF containing MTLF or in ADRF. If the model is stored in ADRF, this message may also contain ADRF ID.

 If the ML model is to be retrieved from ADRF, the following steps are applied:

 8a. NF Service Consumer requests an access token from the NRF to be authorized to retrieve the model stored in ADRF as specified in clause 13.4.1.

 8b. NRF verifies that the NF Service consumer e.g., NWDAF containing AnLF is authorized to access the service provided by the ADRF. If verification is successful, NRF grants the token (token2), based on the information provided in ADRF's NF profile.

 9. NF Service consumer e.g., NWDAF containing AnLF requests to retrieve the target model by sending Nadrf\_MLModelManagement\_Retrieval Request as described in clause 10.3.4 TS 23.288 [105], including token2.

 10. ADRF authenticates the NF Service Consumer and verifies the access token (token2) as specified in the clause 13.4.1.1.2. ADRF verifies also the NF Service Consumer’s NF ID is included in the allowed NF instance list for the ML model and/or is same as the NF ID of the MTLF that stored the model. If verification is successful, ADRF sends Nadrf\_MLModelManagement\_Retrieval Response to the NF Service Consumer, which contains the address of the stored model in ADRF.

 11. NF Service Consumer retrieves the ML model from ADRF and decrypts the model per the vendor’s implementation.

\*\*\* END CHANGES \*\*\*

\*\*\* BEGIN CHANGES \*\*\*

#### 13.4.1.0 General

The authorization framework described in clause 13.4.1 allows NF Service Producers to authorize the requests from NF Service requestors. Subscription requests are considered as service requests.

The authorization framework uses the OAuth 2.0 framework as specified in RFC 6749 [43]. Grants shall be of the type Client Credentials Grant, as described in clause 4.4 of RFC 6749 [43]. Access tokens shall be JSON Web Tokens as described in RFC 7519 [44] and are secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45].

NOTE 1a: Securing the access token using Message Authentication Codes (MAC) based on JSON Web Signature (JWS) as described in RFC 7515 [45] requires a pairwise pre-shared symmetric key between the NRF and the NF Service Producer. The provisioning of such pre-shared symmetric key is outside the scope of this document.

The basic extent provided by the authorization token is at service level (i.e. the "scope" claim includes allowed services per NF type). Depending on the NF Service Producer configuration, higher level of granularity for the authorization token can be defined adding "additional scope" information within the token e.g. to authorize specific service operations and/or resources/data sets within service operations per NF Service Consumer type.

NOTE 1: The additional scope(s) included within the access token add additional security checks at the NF Service Producer that authorizes the services operations, resources and NF Service Consumer type related to the additional scope(s).

The authorization framework described in clause 13.4.1 is mandatory to support for NRF and NF.

The OAuth 2.0 framework does not apply to the notification operation.

Extensions to the authorization framework specific for the security of enablers for Network Automation by 5GS are described in Annex X.

\*\*\* END CHANGES \*\*\*